Larry A. Hammond, 004049
Anne M. Chapman, 025965
OSBORN MALEDON, P.A.
2929 N. Central Avenue, 21st Floor
Phoenix, Arizona 85012-2793
(602) 640-9000
lhammond@omlaw.com
achapman@omlaw.com

John M. Sears, 005617
P.O. Box 4080
Prescott, Arizona 86302
(928) 778-5208
John.Sears@azbar.org

Attorneys for Defendant

IN THE SUPERIOR COURT OF THE STATE OF ARIZONA
IN AND FOR THE COUNTY OF YAVAPAI

STATE OF ARIZONA,	)	No. P1300CR20081339
	)	
Plaintiff,	)	Div. 6
	)	
vs.	)	**REPLY IN SUPPORT OF MOTION TO PRECLUDE LATE DISCLOSED EVIDENCE, RECONSTRUCTION AND OPINIONS FROM THE STATE'S 50-54th DISCLOSURES**
STEVEN CARROLL DEMOCKER,	)	
Defendant.	)	
	)	
	)	(Oral Argument Requested)

The State's response continues to minimize its serious disclosure violations, fails to provide any good cause for those violations and does not cure the extreme prejudice its failures have caused to the defense. We are now three weeks from trial and the State continues to provide late disclosures in violation of this Court's orders and Rule 15.

The Court should preclude the evidence disclosed to the defense on March 2, 17, 19, 24, and 25, 2010.

The State's response presumes that the Court's sanction of striking the F(2) and (6) aggravators addressed all of the State's disclosure violations for all time. The Court's order did not address the disclosure violations outlined in the defense motion regarding these late disclosures, as they had yet to be fully briefed and argued or those motions that are forthcoming based on the State's continued late disclosure. With just weeks to trial, the State continues to late disclose evidence and has not provided any good cause for these failures. Rule 15.7 requires the Court to consider the timing of disclosures in imposing a sanction. As the trial date looms, preclusion is a more appropriate remedy.

1. Sergeant Dan Winslow Reconstruction and Shoe Print Comparison (19762-3)

The State again attempts to invoke its continuing duty to investigate to excuse its failure to engage in basic measurement taking at the scene at the time of the murder and to instead perform and disclose purported measurements seventeen months after Ms. Kennedy's death. With all respect to Sgt. Winslow, measurements taken seventeen months after an event are in no way reliable. This is yet another example of the State's failure to exercise due diligence to take measurements at the scene when it should have, and later attempts to excuse its failures by invoking its duty to investigate. The State did have a duty to investigate. It failed to exercise that duty by taking basic scene measurements. An attempt to take such measurements seventeen months later should be precluded based on its inherent unreliability, and on the State's failure to exercise the due diligence required under Rule 15.1 and this Court's Orders.

Likewise, while it may be appropriate for Sgt. Winslow to refresh his recollection about the presence or absence of shoe prints at the scene by looking at photos, it is certainly beyond merely refreshing his recollection, as well as beyond his disclosed expertise, to engage in photo comparison and attempted identification of shoe prints. Sgt. Winslow's supplemental report after his defense interview is not an attempt to remember whether or not shoe prints are present. Rather, it is an attempt to compare shoes prints from different photos. This is not testimony permitted under Rule 701 and requires expertise that Sgt. Winslow does not possess. The State's attempt to back-door this kind of comparison evidence in should be precluded by the Court based on its prohibition under Rule 701, its late disclosure, and on the lack of foundation for Sgt. Winslow to offer this kind of testimony.

2. Commander Mascher Report on Shoe Print Comparison (19764)

Cmdr. Mascher's supplemental report is not based on personal observation, as suggested by the State's response. Rather, it is based on experiments undertaken by Cmdr. Mascher that he is not trained to perform or evaluate. His report purports to compare a sample shoe from La Sportiva (which the defense has not received) to a photo of a shoe print from the crime scene. He then tries to draw conclusions based on his comparison about the heel patterns on the shoes and about the size of the prints from the photos at the crime scene. Cmdr. Mascher also describes an examination he conducted by tracing tread patterns from the sample shoe and comparing them to photographs from the crime scene and to again draw conclusions about comparing the prints to the sample shoe. These are **not** "personal observations" of the kind of testimony permitted under Rule 701. These are scientific experiments and tests for which the State has late disclosed an expert, Erik Gilkerson. Cmdr. Mascher is not qualified as an expert in shoe print comparison. His attempts to perform tests and experiments on the sample shoes and compare them to photographs is not admissible under Rule 701 as a personal observation as suggested in the State's response. This is yet another attempt by the State to bolster its otherwise meager comparison evidence on shoe prints. The State has disclosed (albeit late) a shoe print expert and should not be permitted to improperly admit additional opinions from unqualified lay witnesses about shoe print comparison as it is attempting to do through Cmdr. Mascher – particularly when this information is disclosed with only a few weeks to trial, and after the defense interview.

3. DPS Computer Forensic Examinations (CDs 6210, 6221, 6222, 6223, 6224, 6225, 6228 and 19810-11)

The State incorrectly responds that the Court has held that the State's late disclosed DPS Computer Forensic Examinations are not precluded. The defense did not understand this Court's April 8, 2010 sanction to be inclusive of all unargued disclosure violations made by the State. This particular late disclosure is particularly prejudicial and inexcusable. On March 2 and March 17, 2010, the State provided the defense with a total of seven CDs from Arizona DPS relating to computer forensic examination of electronic data that has been in the State's possession since July of 2008.

While it is true that these examinations take time, these examinations were not even requested until February and March of 2010. With respect to the particular reports on the recently disclosed CDs, CDs 6224, 6228 and 6222, the reports themselves note that the examination was not even requested until February of 2010. The report on CD 6221 also states that item 1504 was not processed until January 2010. These reports are attached and indicate the date the examination was requested. These items have been in the possession of the State since July of 2008. The State's failure to request examination until mere months before trial is a failure of due diligence and is not explained by the length of time to perform computer forensic examinations. This newly disclosed evidence contains over 8500 pages of reports and emails.

An additional 5 CDs of DPS Computer Forensic disclosure were provided to the defense on April 1, 2010. These CDs were labeled 4, 6249, 6250, 6251, and 6252. These CDs contain over 60,000 pages of reports and emails. Each of these reports indicate that they were **requested by the Yavapai County Attorney on March 16, 2010**. (Attached). The computer at issue in item 4 has been in the possession of the State since October of 2009, for all other CDs, the computers have been in the possession of the State since July of 2008. The State waited until six weeks before trial to even request the examinations that resulted in disclosure of approximately 70,000 pages to the defense. This is not the exercise of due diligence. Nor is it the appropriate time to conduct computer forensic examinations.

The prejudice to the defense cannot be overstated. There have been serious questions as to the reliability of the extraction of the data by the State. The State has used an unqualified non-expert to perform most of the extraction and examination of these items. The State did not remove the power source from one of the items and caused destruction of some of the files. The State has also never provided the defense with the requested EnCase files. This evidence should be excluded by the Court based on its late and incomplete disclosure and based on the State's interference with Mr. DeMocker's Sixth Amendment right to confront this evidence.

4. La Sportiva Information (19665-19675, 19765-19767, 19812 & CD WW)

While the Court's sanction of April 8 did not preclude previously disclosed shoe print information, on March 17, 2010, the State disclosed additional information regarding La Sportiva shoes. This includes information that appears to be from a website, information about sample shoes that were sent to the State (but not provided to the defense), further discussion between the State and a late disclosed expert, a CD of photos, and sales data regarding certain shoes.

At least with respect to the examination of the sample shoe that was not and still has not been provided to the defense, this information and any examination or results from this examination should be excluded. These shoes are no longer for sale, the defense has not had similar access to these sample shoes and has not been able to perform any independent examination, testing or comparisons of this item. Given that trial is just three weeks away and the state has still not provided this evidence to the defense, any comparisons, examination, testimony or results from these sample shoes should be precluded under Rule 15.7.

5. Jail Visit Recordings

The State is again attempting to manipulate this Court and avoid both Rule 15.1 and this Court's Orders with respect to the notice requirements for Mr. DeMocker's statements it intends to rely on at trial. The Court previously ordered the State to identify with particularity, as required under Rule 15.1, what statements of Mr. DeMocker's it intends to use at trial. For statements made before December 31, 2009 the Court ordered the State to make the disclosure by February 6, 2010. For calls through January, the Court ordered the State to make the disclosure by February 13. The State did not identify any jail calls on the dates ordered by the Court. Instead it disclosed over 1000 summaries of jail calls both in supplemental police reports and on CDs and over 2700 jail calls. These summaries do not identify any statements as those the State intends to use at trial. The reports are entitled "Call Summaries." These summaries had been generated as early as 2008 but were not disclosed to the defense until January, 2010. The State later asserted that the defense should have somehow been able to divine that the summaries from police reports as opposed to those produced on CD were those statements it intended to rely on at trial. That is ridiculous. The State failed to do what it was ordered to do by the Court and what Rule 15 requires of it. The State should be precluded from relying on statements it failed to properly notice.

However, even if the State had properly identified the statements in the reports, which it did not do, the State did not do so in the time required by this Court's order. The State responds that it made disclosures on March 3 and April 5 of calls it intends to rely on. The calls from the March 3 "Call Summaries" are from November 2009 and

January 2010. This is in direct defiance of the Court's order requiring disclosure in January and February and these statements should be precluded based on their late disclosure. The April 5 "Call Summaries" include November 2009 calls and January 2010 calls which are both disclosed well past the Court's deadlines and those statements should likewise be excluded. Additionally, one of the statements disclosed on this April 5 summary is from a February visitation that is being listened in on by the State. No recording from this February visitation has been provided to the defense. The State should not be permitted to make use of Mr. DeMocker's statements from visitation rooms for which it has not provided a recording to the defense. And none of these statements should be permitted to be introduced because they were not properly identified as statements the State intends to rely upon under Rule 15.1 or this Court's orders and they are not relevant.

Furthermore, the State provided a list of people to whom statements may have been made and asserted that it intends to rely on statements made by Mr. DeMocker to a list of 16 people. The list does not identify what statements were allegedly made on what date to what person. This does not comply with the notice requirement under Rule 15.1 or the Orders of this Court.

On March 17, 2010, the State disclosed three CDs of recorded jail visits of Mr. DeMocker from January of 2010. No summaries or reports of these visits have been disclosed. It is clear from other disclosure that additional jail visits have been recorded but have not been provided to the defense.

This Court should order that the State is prohibited from relying on any statements other than those it properly identified, those that Mr. DeMocker made to law enforcement on two occasions.

6. Sorenson Forensic Testing (19814-19815 and 19870-19873)

The State's response that a defense expert was present for testing does not address that it has now disclosed testing on four individuals about whom no other disclosure was provided. The defense expert was not provided with any information regarding these individuals nor was the testing for which the defense expert was present related in any way to these individuals. There are no police reports about or referring to these individuals and no interviews of or referring to these individuals. The defense has no idea why these individuals are being tested now, with less than six weeks to trial. This information should be excluded based on the State's failure to provide disclosure to the defense pursuant to Rule 15.7.

7. FIA Card Services (Bates 18985-19045) and Provident Funding Documents (19364-19655)

Although the State is correct that the Court noted that some delay in obtaining bank records was understandable, we are now three weeks away from trial. At some point, the State must stop. The FIA bank account information disclosed in March was known to the state as of December of 2008.

The Provident mortgage was known to the State at least as early as November 2008. Yet the State did not subpoena the information until March of 2010. This information should be excluded pursuant to Rule 15.7.

8. Phone Records (19267-19363, 19828-19860)

At the very least, the State acknowledges that it was aware in June 2009 that it needed to obtain these records that it did not subpoena and disclose until March of 2010. On its face this is yet another failure of the State's duty of due diligence. The State waited almost a year to request and disclose these phone records. This is particularly true where the State also failed to disclose the phone call summaries that generated interest in this information to the defense until January of 2010. This information should be precluded by the Court based on its late disclosure and the State's withholding of jail call summaries between 2008 and 2010.

9. Purchases from February 2008 (19821-19827) and New Witness

Counsel received an email on April 11 from Ms. Butler that copied Mr. Butner indicating that Ms. Butler believed that Mr. DeMocker may have been in Ms. Kennedy's home to leave flowers on Valentine's day of 2007, almost a year and a half before Ms. Kennedy was murdered. The State has not disclosed any communication with Ms. Butler in the last 30 days regarding communication about when this event occurred. The State knew of this transaction as of November of 2008. (Bates 1353). Apparently, the State thinks that this "evidence" will somehow allow them to argue the absurd proposition that if Mr. DeMocker was in Carol's home on Valentine's Day to leave her flowers a year and half earlier, then he must have been in her home on July 2, 2010 to kill her. This evidence was not timely disclosed and, in any case is not relevant and should be excluded on this basis or, alternatively, under Rule 403.

CONCLUSION

The Court should exclude the above described evidence based on its late disclosure. The evidence was known to the State months, and in some cases well over a year, before it was disclosed to the defense. The State failed to exercise due diligence to request and disclose the evidence to the defense. The State has not offered any good cause for its failure to exercise due diligence. The late disclosure has prejudiced the defense's ability to prepare for trial and confront the evidence, as outlined above and in prior motions. The evidence should therefore be excluded pursuant to Rule 15.7.

Defendant Steven DeMocker, by and through counsel, hereby requests that this Court prohibit the State from offering late disclosed evidence, reconstructions and opinions as described above.

DATED this 12TH day of April, 2010.

By: ______________________
John M. Sears
P.O. Box 4080
Prescott, Arizona 86302

OSBORN MALEDON, P.A.
Larry A. Hammond
Anne M. Chapman
2929 N. Central Avenue, Suite 2100
Phoenix, Arizona 85012-2793

Attorneys for Defendant

ORIGINAL of the foregoing hand delivered for filing this 12th day of April, 2010, with:

Jeanne Hicks
Clerk of the Court
Yavapai County Superior Court
120 S. Cortez
Prescott, AZ 86303

COPIES of the foregoing hand delivered this this 12th day of April, 2010, to:

The Hon. Thomas B. Lindberg
Judge of the Superior Court
Division Six
120 S. Cortez
Prescott, AZ 86303

Joseph C. Butner, Esq.
Prescott Courthouse basket

____

Yavapai County Sheriff's Office
Criminal Investigations Bureau
Computer Forensic Examination Report

AGENCY:	YAVAPAI COUNTY SHERIFF'S OFFICE
AGENCY DR#:	08-029129
CFU #:	P0261
DPS EVIDENCE DR#:	2008-723747
INVESTIGATOR:	DETECTIVE JOHN MCDORMETT #5472
EXAMINER:	DETECTIVE STEVE PAGE #5430
REPORT DATE:	MARCH 3, 2010

REQUESTED EXAMINATION:

Detective Page was assigned by Lieutenant David Rhodes, Yavapai County Sheriff's Office Criminal Investigations Bureau, to work at the DPS Regional Computer Forensic Lab to conduct the forensic processing and examination of the below listed items for information related to the investigation of the homicide of Virginia Carol Kennedy.

Item #	Description	Model No.	Serial No.
1504	Apple Time Capsule 802.11n Wi-Fi HD	A1254	6F818B9MYZV
	Containing one (1) Seagate Barracuda ES 500.0GB HD	ST3500630NS	5QG2XHJ6

INSPECTION & ACQUISITION:

COMPLETED BY: Detective Page

1. The above listed item was obtained from DPS Property and Evidence and delivered to the Arizona Regional Computer Forensics Lab by Sergeant Arthur on 12/10/2009.

2. On 12/14/09 Detective Page was assigned to process evidence item 1504. The item was processed on 1/04/10. The hard drive was removed from the item and was connected to a government computer via a Digital Intelligence UltraBlock hardware write blocker to prevent any alterations to the source media during imaging. Guidance Software's EnCase 6 forensic software program was used to acquire a forensic image. The imaging process completed successfully with matching acquisition and verification MD5 hash values. The item was photographed to document packaging, unit labeling and write blocker connections.

PROCEDURE:

The image of item 1504 was examined using EnCase 6. The hard drive device information was documented in the "Item 1504 Drive Data" report. The hard drive was divided into three partitions named: "1 APconfig", "2 APswap", and "3 APdata". The partition information was copied from EnCase and can be viewed in the "Item 1504 Partition Data" report.

EXAMINATION FINDINGS:

Item 1504: Each partition contained system files only. The hard drive appeared to have been initialized (prepared for use), but did not have any user files stored on it. No items of evidentiary value were located.

Steve Page #5430

Detective Steve Page, #5430
Yavapai County Sheriff's Office
Criminal Investigations Bureau

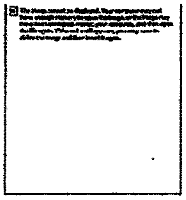
Peer Review:

The above listed report was peer reviewed for technical accuracy and content. The results listed in this report were reviewed with Detective Page to verify the statements made in this report accurately portray the forensic findings found using EnCase.

Paul Lindvay #5497

Detective P. A. Lindvay, #5497
AZ Department Of Public Safety
Computer Forensic Unit

Yavapai County Sheriff's Office
Criminal Investigations Bureau
Computer Forensic Examination Report



AGENCY:	YAVAPAI COUNTY SHERIFF'S OFFICE
AGENCY DR#:	08-029129
CFU #:	P0261
DPS EVIDENCE DR#:	2008-723747
INVESTIGATOR:	DETECTIVE JOHN MCDORMETT #5472
EXAMINER:	DETECTIVE STEVE PAGE #5430
REPORT DATE:	MARCH 3, 2010

REQUESTED EXAMINATION:

Detective Page was assigned by Lieutenant David Rhodes, Yavapai County Sheriff's Office Criminal Investigations Bureau, to work at the DPS Regional Computer Forensic Lab to conduct the forensic processing and examination of the below listed items for information related to the investigation of the homicide of Virginia Carol Kennedy.

Item #	Description	Model No.	Serial No.
1504	Apple Time Capsule 802.11n Wi-Fi HD	A1254	6F818B9MYZV
	Containing one (1) Seagate Barracuda ES 500.0GB HD	ST3500630NS	5QG2XHJ6

INSPECTION & ACQUISITION:

COMPLETED BY: Detective Page

1. The above listed item was obtained from DPS Property and Evidence and delivered to the Arizona Regional Computer Forensics Lab by Sergeant Arthur on 12/10/2009.

2. On 12/14/09 Detective Page was assigned to process evidence item 1504. The item was processed on 1/04/10. The hard drive was removed from the item and was connected to a government computer via a Digital Intelligence UltraBlock hardware write blocker to prevent any alterations to the source media during imaging. Guidance Software's EnCase 6 forensic software program was used to acquire a forensic image. The imaging process completed successfully with matching acquisition and verification MD5 hash values. The item was photographed to document packaging, unit labeling and write blocker connections.

PROCEDURE:

The image of item 1504 was examined using EnCase 6. The hard drive device information was documented in the "Item 1504 Drive Data" report. The hard drive was divided into three partitions named: "1 APconfig", "2 APswap", and "3 APdata". The partition information was copied from EnCase and can be viewed in the "Item 1504 Partition Data" report.

EXAMINATION FINDINGS:

Item 1504: Each partition contained system files only. The hard drive appeared to have been initialized (prepared for use), but did not have any user files stored on it. No items of evidentiary value were located.

Detective Steve Page, #5430
Yavapai County Sheriff's Office
Criminal Investigations Bureau

Peer Review:

The above listed report was peer reviewed for technical accuracy and content. The results listed in this report were reviewed with Detective Page to verify the statements made in this report accurately portray the forensic findings found using EnCase.

Detective P. A. Lindvay, #5497
AZ Department Of Public Safety
Computer Forensic Unit

Yavapai County Sheriff's Office
Criminal Investigations Bureau
Computer Forensics Unit

Extracted Data Documentation

AGENCY: Yavapai County Sheriff's Office
AGENCY DR#: 08-029129
CFU #: P0261
DPS Evidence DR#: 2008-723747
INVESTIGATOR: DETECTIVE JOHN MCDORMETT #5472
EXAMINER: DETECTIVE STEVE PAGE #5430
DATE: MARCH 4, 2010

#6222

REQUESTED EXAMINATION:

On 2/03/10 Deputy County Attorney Joe Butner requested that Detective Page extract emails between Steven DeMocker and Carol Kennedy, between the dates of January 1, 2007 and July 3, 2008, from DeMocker's laptop computer (Item 411) and Kennedy's computer (Item 513). Mr. Butner also requested that Detective Page extract emails between Steven DeMocker and Barbara O'Non, between the dates of January 1, 2007 and October 23, 2008, from DeMocker's laptop computer (Item 411). Mr. Butner requested that the extracted emails be grouped by the evidence item from which they were found, and to provide the extracted emails to Detective McDormett for further analysis.

On 2/09/10 Joe Butner requested that Detective Page also extract emails between Steven DeMocker and Barbara O'Non, between the dates of January 1, 2007 and October 23, 2008, from DeMocker's UBS/work computer (Item 301).

Evidence Items:

Item #	Description	Model No.	Serial No.
301	Dell Optiplex 745 computer, containing: One (1) Seagate Barracuda 160 GB SATA HDD	DCCY ST3160812AS	7P23SD1 5LSH1KS3
411	IBM ThinkPad Laptop, containing: One (1) Fujitsu 60.0 GB SATA HDD	2623-D9U MHV2060BH	L3-A9400 NW06T6425FN9
513	IBM ThinkCentre Computer, containing: One (1) Hitachi Deskstar 80.0 GB ATA HDD Serial No.: 11S07N9675Z1Z7NNDAPHZT	43U IC35L090AVV207-0	KCAM93C

PROCEDURES:

General Procedures:

Guidance Software's EnCase 6 forensic program was used to process the evidence for this request. The results of a search for email records previously run in EnCase were used for this examination. That search was documented in the 012910 Computer Evidence Forensic Report (Procedure section, under "General Email Searches", 4th paragraph).

One of the processes available in EnCase to filter data for more efficient examination is called 'Conditions'. Conditions available for examining email data include filtering on the "From" and "To" email attributes. To run a condition, the examiner must specify the information (called an 'expression') to find in the data, and when run, the condition will show only entries containing that expression. For this examination, both the "From Contains…" and "To Contains…" conditions were utilized. When both conditions are applied together, email entries can be filtered to show only those emails between specific persons. Detective Page reviewed email addresses in the 'To' and 'From' attributes of the email data to identify appropriate expressions to use in conditions.

The following expressions were developed to filter email for each respective person:

DeMocker:

se04788
steven.democker
DeMocker, Steven
sdem
democker@cableone.net
Este

Kennedy:

carolkennedy
ckennedy
virginiacarolkennedy
carolita
carol kennedy

O'Non:

be02465
Barbara.onon
O'Non, Barbara
Barbara O'Non
Barbara Onon
Bonon
o'non

Specific Procedures:

A) Email between DeMocker & Kennedy, 1/01/2007 – 7/03/2008, from Item 411

The EnCase 'Set Include' function was used to select all email records for Item 411 in the Records tab.

The expressions for DeMocker were entered into the "From Contains…" condition, and the condition run. Then the expressions for Kennedy were entered into the "To Contains…" condition, and the condition run. The resulting entries listed all the email in Item 411 *from* DeMocker *to* Kennedy. The entries were then sorted by date and entries lying within the specified dates were checked (tagged) for later reference. The current conditions were then cancelled, allowing all the email to again be listed, but leaving the selected entries checked.

Next, the expressions for Kennedy were entered into the "From Contains…" condition, and the condition run. Then the expressions for DeMocker were entered into the "To Contains…" condition, and the condition run. The resulting entries listed all the email in Item 411 *from* Kennedy *to* DeMocker. The entries were then sorted by date and entries lying within the specified dates were checked for later reference, and the current conditions were then cancelled. Note that this process simply reversed the first conditions noted above.

This process resulted in a list in which all the emails between DeMocker and Kennedy, on or between the specified dates, were checked. Those selected emails were exported from EnCase as Outlook message files (.msg or MSG).

The exported MSG files were then imported into Outlook 2003. Outlook stores emails, contacts, appointments and other items in a data file called a personal storage file (.pst or PST). A PST file was created to contain the above-selected emails, and given the name "Item 411 SD-CK Email Jan07-Jul08.pst". The PST file format was chosen so that the requested email files can be efficiently provided to, and analyzed by, other investigators involved in the case.

The above described process was repeated for each of the remaining requested examinations, modified for the respective dates, persons and Evidence Item. The PST file produced for each is noted below.

B) Email between DeMocker & Kennedy, 1/01/2007 – 7/03/2008, from Item 513
PST file name: Item 513 SD-CK Email Jan07-Jul08.pst.

C) Email between DeMocker & O'Non, 1/01/2007 – 10/23/2008, from Item 411
PST file name: Item 411 SD-Onon Email Jan07-Oct08.pst;

D) Email between DeMocker & O'Non, 1/01/2007 – 10/23/2008, from Item 301
PST file name: Item 301 SD-Onon Email Jan07-Oct08.pst;

The Outlook PST data files were then copied to CD discs. The Item 301 PST SD-Onon Email PST file was copied to its own CD disc; the Item 411 SD-Onon Email PST file was copied to its own CD disc; and the two PST files containing emails between DeMocker and Kennedy (SD-CK) were placed on a third CD disc. The discs were provided to Det. McDormett for further analysis.

Steve Page #5430

Detective Steve Page, #5430
Yavapai County Sheriff's Office
Criminal Investigations Bureau

Peer Review:

The above listed report was peer reviewed for technical accuracy and content. The results listed in this report were reviewed with Detective Page to verify the statements made in this report accurately portray the forensic findings found using EnCase.

Paul Lindvay #5497

Detective P. A. Lindvay, #5497
AZ Department Of Public Safety

Yavapai County Sheriff's Office
Criminal Investigations Bureau
Computer Forensics Unit

Extracted Data Documentation

AGENCY:	Yavapai County Sheriff's Office
AGENCY DR#:	08-029129
CFU #:	P0261
DPS Evidence DR#:	2008-723747
INVESTIGATOR:	DETECTIVE JOHN MCDORMETT #5472
EXAMINER:	DETECTIVE STEVE PAGE #5430
DATE:	MARCH 4, 2010

REQUESTED EXAMINATION:

On 2/03/10 Deputy County Attorney Joe Butner requested that Detective Page extract emails between Steven DeMocker and Carol Kennedy, between the dates of January 1, 2007 and July 3, 2008, from DeMocker's laptop computer (Item 411) and Kennedy's computer (Item 513). Mr. Butner also requested that Detective Page extract emails between Steven DeMocker and Barbara O'Non, between the dates of January 1, 2007 and October 23, 2008, from DeMocker's laptop computer (Item 411). Mr. Butner requested that the extracted emails be grouped by the evidence item from which they were found, and to provide the extracted emails to Detective McDormett for further analysis.

On 2/09/10 Joe Butner requested that Detective Page also extract emails between Steven DeMocker and Barbara O'Non, between the dates of January 1, 2007 and October 23, 2008, from DeMocker's UBS/work computer (Item 301).

Evidence Items:

Item #	Description	Model No.	Serial No.
301	Dell Optiplex 745 computer, containing:	DCCY	7P23SD1
	One (1) Seagate Barracuda 160 GB SATA HDD	ST3160812AS	5LSH1KS3
411	IBM ThinkPad Laptop, containing:	2623-D9U	L3-A9400
	One (1) Fujitsu 60.0 GB SATA HDD	MHV2060BH	NW06T6425FN9
513	IBM ThinkCentre Computer, containing:	43U	KCAM93C
	One (1) Hitachi Deskstar 80.0 GB ATA HDD	IC35L090AVV207-0	
	Serial No.: 11S07N9675Z1Z7NNDAPHZT		

PROCEDURES:

General Procedures:

Guidance Software's EnCase 6 forensic program was used to process the evidence for this request. The results of a search for email records previously run in EnCase were used for this examination. That search was documented in the 012910 Computer Evidence Forensic Report (Procedure section, under "General Email Searches", 4th paragraph).

One of the processes available in EnCase to filter data for more efficient examination is called 'Conditions'. Conditions available for examining email data include filtering on the "From" and "To" email attributes. To run a condition, the examiner must specify the information (called an 'expression') to find in the data, and when run, the condition will show only entries containing that expression. For this examination, both the "From Contains..." and "To Contains..." conditions were utilized. When both conditions are applied together, email entries can be filtered to show only those emails between specific persons. Detective Page reviewed email addresses in the 'To' and 'From' attributes of the email data to identify appropriate expressions to use in conditions.

The following expressions were developed to filter email for each respective person:

DeMocker:
se04788
steven.democker
DeMocker, Steven
sdem
democker@cableone.net
Estc

Kennedy:
carolkennedy
ckennedy
virginiacarolkennedy
carolita
carol kennedy

O'Non:
be02465
Barbara.onon
O'Non, Barbara
Barbara O'Non
Barbara Onon
Bonon
o'non

Specific Procedures:

A) Email between DeMocker & Kennedy, 1/01/2007 – 7/03/2008, from Item 411

The EnCase 'Set Include' function was used to select all email records for Item 411 in the Records tab.

The expressions for DeMocker were entered into the "From Contains .." condition, and the condition run. Then the expressions for Kennedy were entered into the "To Contains..." condition, and the condition run. The resulting entries listed all the email in Item 411 *from* DeMocker *to* Kennedy. The entries were then sorted by date and entries lying within the specified dates were checked (tagged) for later reference. The current conditions were then cancelled, allowing all the email to again be listed, but leaving the selected entries checked.

Next, the expressions for Kennedy were entered into the "From Contains..." condition, and the condition run. Then the expressions for DeMocker were entered into the "To Contains.. " condition, and the condition run. The resulting entries listed all the email in Item 411 *from* Kennedy *to* DeMocker. The entries were then sorted by date and entries lying within the specified dates were checked for later reference, and the current conditions were then cancelled. Note that this process simply reversed the first conditions noted above.

This process resulted in a list in which all the emails between DeMocker and Kennedy, on or between the specified dates, were checked. Those selected emails were exported from EnCase as Outlook message files (.msg or MSG).

The exported MSG files were then imported into Outlook 2003. Outlook stores emails, contacts, appointments and other items in a data file called a personal storage file (.pst or PST). A PST file was created to contain the above-selected emails, and given the name "Item 411 SD-CK Email Jan07-Jul08.pst". The PST file format was chosen so that the requested email files can be efficiently provided to, and analyzed by, other investigators involved in the case.

The above described process was repeated for each of the remaining requested examinations, modified for the respective dates, persons and Evidence Item. The PST file produced for each is noted below.

B) Email between DeMocker & Kennedy, 1/01/2007 – 7/03/2008, from Item 513
PST file name: Item 513 SD-CK Email Jan07-Jul08.pst.

C) Email between DeMocker & O'Non, 1/01/2007 – 10/23/2008, from Item 411
PST file name: Item 411 SD-Onon Email Jan07-Oct08.pst;

D) Email between DeMocker & O'Non, 1/01/2007 – 10/23/2008, from Item 301
PST file name: Item 301 SD-Onon Email Jan07-Oct08.pst;

The Outlook PST data files were then copied to CD discs. The Item 301 PST SD-Onon Email PST file was copied to its own CD disc; the Item 411 SD-Onon Email PST file was copied to its own CD disc; and the two PST files containing emails between DeMocker and Kennedy (SD-CK) were placed on a third CD disc. The discs were provided to Det. McDormett for further analysis.

Steve Page #5430

Detective Steve Page, #5430
Yavapai County Sheriff's Office
Criminal Investigations Bureau

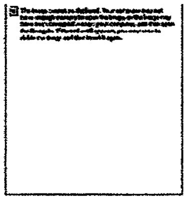
Peer Review:

The above listed report was peer reviewed for technical accuracy and content. The results listed in this report were reviewed with Detective Page to verify the statements made in this report accurately portray the forensic findings found using EnCase.

Paul Lindvay #5497

Detective P. A. Lindvay, #5497
AZ Department Of Public Safety

Yavapai County Sheriff's Office
Criminal Investigations Bureau
Computer Forensics Unit



Extracted Data Documentation

AGENCY:	Yavapai County Sheriff's Office
AGENCY DR#:	08-029129
CFU #:	P0261
DPS Evidence DR#:	2008-723747
INVESTIGATOR:	DETECTIVE JOHN MCDORMETT #5472
EXAMINER:	DETECTIVE STEVE PAGE #5430
DATE:	MARCH 4, 2010

REQUESTED EXAMINATION:

On 2/03/10 Deputy County Attorney Joe Butner requested that Detective Page extract emails between Steven DeMocker and Carol Kennedy, between the dates of January 1, 2007 and July 3, 2008, from DeMocker's laptop computer (Item 411) and Kennedy's computer (Item 513). Mr. Butner also requested that Detective Page extract emails between Steven DeMocker and Barbara O'Non, between the dates of January 1, 2007 and October 23, 2008, from DeMocker's laptop computer (Item 411). Mr. Butner requested that the extracted emails be grouped by the evidence item from which they were found, and to provide the extracted emails to Detective McDormett for further analysis.

On 2/09/10 Joe Butner requested that Detective Page also extract emails between Steven DeMocker and Barbara O'Non, between the dates of January 1, 2007 and October 23, 2008, from DeMocker's UBS/work computer (Item 301).

Evidence Items:

Item #	Description	Model No.	Serial No.
301	Dell Optiplex 745 computer, containing: One (1) Seagate Barracuda 160 GB SATA HDD	DCCY ST3160812AS	7P23SD1 5LSH1KS3
411	IBM ThinkPad Laptop, containing: One (1) Fujitsu 60.0 GB SATA HDD	2623-D9U MHV2060BH	L3-A9400 NW06T6425FN9
513	IBM ThinkCentre Computer, containing: One (1) Hitachi Deskstar 80.0 GB ATA HDD Serial No.: 11S07N9675Z1Z7NNDAPHZT	43U IC35L090AVV207-0	KCAM93C

PROCEDURES:

General Procedures:

Guidance Software's EnCase 6 forensic program was used to process the evidence for this request. The results of a search for email records previously run in EnCase were used for this examination. That search was documented in the 012910 Computer Evidence Forensic Report (Procedure section, under "General Email Searches", 4th paragraph).

One of the processes available in EnCase to filter data for more efficient examination is called 'Conditions'. Conditions available for examining email data include filtering on the "From" and "To" email attributes. To run a condition, the examiner must specify the information (called an 'expression') to find in the data, and when run, the condition will show only entries containing that expression. For this examination, both the "From Contains…" and "To Contains…" conditions were utilized. When both conditions are applied together, email entries can be filtered to show only those emails between specific persons. Detective Page reviewed email addresses in the 'To' and 'From' attributes of the email data to identify appropriate expressions to use in conditions.

The following expressions were developed to filter email for each respective person:

DeMocker:	**Kennedy:**	**O'Non:**
se04788	carolkennedy	be02465
steven.democker	ckennedy	Barbara.onon
DeMocker, Steven	virginiacarolkennedy	O'Non, Barbara
sdem	carolita	Barbara O'Non
democker@cableone.net	carol kennedy	Barbara Onon
Este		Bonon
		o'non

Specific Procedures:

A) Email between DeMocker & Kennedy, 1/01/2007 – 7/03/2008, from Item 411

The EnCase 'Set Include' function was used to select all email records for Item 411 in the Records tab.

The expressions for DeMocker were entered into the "From Contains…" condition, and the condition run. Then the expressions for Kennedy were entered into the "To Contains…" condition, and the condition run. The resulting entries listed all the email in Item 411 *from* DeMocker *to* Kennedy. The entries were then sorted by date and entries lying within the specified dates were checked (tagged) for later reference. The current conditions were then cancelled, allowing all the email to again be listed, but leaving the selected entries checked.

Next, the expressions for Kennedy were entered into the "From Contains…" condition, and the condition run. Then the expressions for DeMocker were entered into the "To Contains.. " condition, and the condition run. The resulting entries listed all the email in Item 411 *from* Kennedy *to* DeMocker. The entries were then sorted by date and entries lying within the specified dates were checked for later reference, and the current conditions were then cancelled. Note that this process simply reversed the first conditions noted above.

This process resulted in a list in which all the emails between DeMocker and Kennedy, on or between the specified dates, were checked. Those selected emails were exported from EnCase as Outlook message files (.msg or MSG).

The exported MSG files were then imported into Outlook 2003. Outlook stores emails, contacts, appointments and other items in a data file called a personal storage file (.pst or PST). A PST file was created to contain the above-selected emails, and given the name "Item 411 SD-CK Email Jan07-Jul08.pst". The PST file format was chosen so that the requested email files can be efficiently provided to, and analyzed by, other investigators involved in the case.

The above described process was repeated for each of the remaining requested examinations, modified for the respective dates, persons and Evidence Item. The PST file produced for each is noted below.

B) Email between DeMocker & Kennedy, 1/01/2007 – 7/03/2008, from Item 513
PST file name: Item 513 SD-CK Email Jan07-Jul08.pst.

C) Email between DeMocker & O'Non, 1/01/2007 – 10/23/2008, from Item 411
PST file name: Item 411 SD-Onon Email Jan07-Oct08.pst;

D) Email between DeMocker & O'Non, 1/01/2007 – 10/23/2008, from Item 301
PST file name: Item 301 SD-Onon Email Jan07-Oct08.pst;

The Outlook PST data files were then copied to CD discs. The Item 301 PST SD-Onon Email PST file was copied to its own CD disc; the Item 411 SD-Onon Email PST file was copied to its own CD disc; and the two PST files containing emails between DeMocker and Kennedy (SD-CK) were placed on a third CD disc. The discs were provided to Det. McDormett for further analysis.

[illegible]

Detective Steve Page, #5430
Yavapai County Sheriff's Office
Criminal Investigations Bureau

Peer Review:

The above listed report was peer reviewed for technical accuracy and content. The results listed in this report were reviewed with Detective Page to verify the statements made in this report accurately portray the forensic findings found using EnCase.

[illegible]

Detective P. A. Lindvay, #5497

Yavapai County Sheriff's Office
Criminal Investigations Bureau
Computer Forensics Unit

Extracted Data Documentation

AGENCY:	Yavapai County Sheriff's Office
AGENCY DR#:	08-029129
CFU #:	P0261
DPS Evidence DR#:	2008-723747
INVESTIGATOR:	DETECTIVE JOHN MCDORMETT #5472
EXAMINER:	DETECTIVE STEVE PAGE #5430
DATE:	MARCH 4, 2010

REQUESTED EXAMINATION:

On 2/03/10 Deputy County Attorney Joe Butner requested that Detective Page extract emails between Steven DeMocker and Carol Kennedy, between the dates of January 1, 2007 and July 3, 2008, from DeMocker's laptop computer (Item 411) and Kennedy's computer (Item 513). Mr. Butner also requested that Detective Page extract emails between Steven DeMocker and Barbara O'Non, between the dates of January 1, 2007 and October 23, 2008, from DeMocker's laptop computer (Item 411). Mr. Butner requested that the extracted emails be grouped by the evidence item from which they were found, and to provide the extracted emails to Detective McDormett for further analysis.

On 2/09/10 Joe Butner requested that Detective Page also extract emails between Steven DeMocker and Barbara O'Non, between the dates of January 1, 2007 and October 23, 2008, from DeMocker's UBS/work computer (Item 301).

Evidence Items:

Item #	Description	Model No.	Serial No.
301	Dell Optiplex 745 computer, containing:	DCCY	7P23SD1
	One (1) Seagate Barracuda 160 GB SATA HDD	ST3160812AS	5LSH1KS3
411	IBM ThinkPad Laptop, containing:	2623-D9U	L3-A9400
	One (1) Fujitsu 60.0 GB SATA HDD	MHV2060BH	NW06T6425FN9
513	IBM ThinkCentre Computer, containing:	43U	KCAM93C
	One (1) Hitachi Deskstar 80.0 GB ATA HDD	IC35L090AVV207-0	
	Serial No.: 11S07N9675Z1Z7NNDAPHZT		

PROCEDURES:

General Procedures:

Guidance Software's EnCase 6 forensic program was used to process the evidence for this request. The results of a search for email records previously run in EnCase were used for this examination. That search was documented in the 012910 Computer Evidence Forensic Report (Procedure section, under "General Email Searches", 4th paragraph).

One of the processes available in EnCase to filter data for more efficient examination is called 'Conditions'. Conditions available for examining email data include filtering on the "From" and "To" email attributes. To run a condition, the examiner must specify the information (called an 'expression') to find in the data, and when run, the condition will show only entries containing that expression. For this examination, both the "From Contains…" and "To Contains…" conditions were utilized. When both conditions are applied together, email entries can be filtered to show only those emails between specific persons. Detective Page reviewed email addresses in the 'To' and 'From' attributes of the email data to identify appropriate expressions to use in conditions.

The following expressions were developed to filter email for each respective person:

DeMocker:

se04788
steven.democker
DeMocker, Steven
sdem
democker@cableone.net
Estc

Kennedy:

carolkennedy
ckennedy
virginiacarolkennedy
carolita
carol kennedy

O'Non:

be02465
Barbara.onon
O'Non, Barbara
Barbara O'Non
Barbara Onon
Bonon
o'non

Specific Procedures:

A) Email between DeMocker & Kennedy, 1/01/2007 – 7/03/2008, from Item 411

The EnCase 'Set Include' function was used to select all email records for Item 411 in the Records tab.

The expressions for DeMocker were entered into the "From Contains .." condition, and the condition run. Then the expressions for Kennedy were entered into the "To Contains…" condition, and the condition run. The resulting entries listed all the email in Item 411 *from* DeMocker *to* Kennedy. The entries were then sorted by date and entries lying within the specified dates were checked (tagged) for later reference. The current conditions were then cancelled, allowing all the email to again be listed, but leaving the selected entries checked.

Next, the expressions for Kennedy were entered into the "From Contains…" condition, and the condition run. Then the expressions for DeMocker were entered into the "To Contains…" condition, and the condition run. The resulting entries listed all the email in Item 411 *from* Kennedy *to* DeMocker. The entries were then sorted by date and entries lying within the specified dates were checked for later reference, and the current conditions were then cancelled. Note that this process simply reversed the first conditions noted above.

This process resulted in a list in which all the emails between DeMocker and Kennedy, on or between the specified dates, were checked. Those selected emails were exported from EnCase as Outlook message files (.msg or MSG).

The exported MSG files were then imported into Outlook 2003. Outlook stores emails, contacts, appointments and other items in a data file called a personal storage file (.pst or PST). A PST file was created to contain the above-selected emails, and given the name "Item 411 SD-CK Email Jan07-Jul08.pst". The PST file format was chosen so that the requested email files can be efficiently provided to, and analyzed by, other investigators involved in the case.

The above described process was repeated for each of the remaining requested examinations, modified for the respective dates, persons and Evidence Item. The PST file produced for each is noted below.

B) Email between DeMocker & Kennedy, 1/01/2007 – 7/03/2008, from Item 513
PST file name: Item 513 SD-CK Email Jan07-Jul08.pst.

C) Email between DeMocker & O'Non, 1/01/2007 – 10/23/2008, from Item 411
PST file name: Item 411 SD-Onon Email Jan07-Oct08.pst;

D) Email between DeMocker & O'Non, 1/01/2007 – 10/23/2008, from Item 301
PST file name: Item 301 SD-Onon Email Jan07-Oct08.pst;

The Outlook PST data files were then copied to CD discs. The Item 301 PST SD-Onon Email PST file was copied to its own CD disc; the Item 411 SD-Onon Email PST file was copied to its own CD disc; and the two PST files containing emails between DeMocker and Kennedy (SD-CK) were placed on a third CD disc. The discs were provided to Det. McDormett for further analysis.

Steve Page #5430

Detective Steve Page, #5430
Yavapai County Sheriff's Office
Criminal Investigations Bureau

Peer Review:

The above listed report was peer reviewed for technical accuracy and content. The results listed in this report were reviewed with Detective Page to verify the statements made in this report accurately portray the forensic findings found using EnCase.

Paul Lindvay #5497

Detective P. A. Lindvay, #5497
AZ Department Of Public Safety

Yavapai County Sheriff's Office
Criminal Investigations Bureau
Computer Forensics Unit

Extracted Data Documentation

AGENCY:	**Yavapai County Sheriff's Office**
AGENCY DR#:	**08-029129**
CFU #:	**P0261**
DPS Evidence DR#:	**2008-723747**
INVESTIGATOR:	**DETECTIVE JOHN MCDORMETT #5472**
EXAMINER:	**DETECTIVE STEVE PAGE #5430**
DATE:	**MARCH 4, 2010**

REQUESTED EXAMINATION:

On 2/03/10 Deputy County Attorney Joe Butner requested that Detective Page extract emails between Steven DeMocker and Carol Kennedy, between the dates of January 1, 2007 and July 3, 2008, from DeMocker's laptop computer (Item 411) and Kennedy's computer (Item 513). Mr. Butner also requested that Detective Page extract emails between Steven DeMocker and Barbara O'Non, between the dates of January 1, 2007 and October 23, 2008, from DeMocker's laptop computer (Item 411). Mr. Butner requested that the extracted emails be grouped by the evidence item from which they were found, and to provide the extracted emails to Detective McDormett for further analysis.

On 2/09/10 Joe Butner requested that Detective Page also extract emails between Steven DeMocker and Barbara O'Non, between the dates of January 1, 2007 and October 23, 2008, from DeMocker's UBS/work computer (Item 301).

Evidence Items:

Item #	Description	Model No.	Serial No.
301	Dell Optiplex 745 computer, containing:	DCCY	7P23SD1
	One (1) Seagate Barracuda 160 GB SATA HDD	ST3160812AS	5LSH1KS3
411	IBM ThinkPad Laptop, containing:	2623-D9U	L3-A9400
	One (1) Fujitsu 60.0 GB SATA HDD	MHV2060BH	NW06T6425FN9
513	IBM ThinkCentre Computer, containing:	43U	KCAM93C
	One (1) Hitachi Deskstar 80.0 GB ATA HDD	IC35L090AVV207-0	
	Serial No.: 11S07N9675Z1Z7NNDAPHZT		

PROCEDURES:

General Procedures:

Guidance Software's EnCase 6 forensic program was used to process the evidence for this request. The results of a search for email records previously run in EnCase were used for this examination. That search was documented in the 012910 Computer Evidence Forensic Report (Procedure section, under "General Email Searches", 4th paragraph).

One of the processes available in EnCase to filter data for more efficient examination is called 'Conditions'. Conditions available for examining email data include filtering on the "From" and "To" email attributes. To run a condition, the examiner must specify the information (called an 'expression') to find in the data, and when run, the condition will show only entries containing that expression. For this examination, both the "From Contains…" and "To Contains…" conditions were utilized. When both conditions are applied together, email entries can be filtered to show only those emails between specific persons. Detective Page reviewed email addresses in the 'To' and 'From' attributes of the email data to identify appropriate expressions to use in conditions.

The following expressions were developed to filter email for each respective person:

DeMocker:	**Kennedy:**	**O'Non:**
se04788	carolkennedy	be02465
steven.democker	ckennedy	Barbara.onon
DeMocker, Steven	virginiacarolkennedy	O'Non, Barbara
sdem	carolita	Barbara O'Non
democker@cableone.net	carol kennedy	Barbara Onon
Este		Bonon
		o'non

Specific Procedures:

A) Email between DeMocker & Kennedy, 1/01/2007 – 7/03/2008, from Item 411

The EnCase 'Set Include' function was used to select all email records for Item 411 in the Records tab.

The expressions for DeMocker were entered into the "From Contains…" condition, and the condition run. Then the expressions for Kennedy were entered into the "To Contains…" condition, and the condition run. The resulting entries listed all the email in Item 411 *from* DeMocker *to* Kennedy. The entries were then sorted by date and entries lying within the specified dates were checked (tagged) for later reference. The current conditions were then cancelled, allowing all the email to again be listed, but leaving the selected entries checked.

Next, the expressions for Kennedy were entered into the "From Contains…" condition, and the condition run. Then the expressions for DeMocker were entered into the "To Contains…" condition, and the condition run. The resulting entries listed all the email in Item 411 *from* Kennedy *to* DeMocker. The entries were then sorted by date and entries lying within the specified dates were checked for later reference, and the current conditions were then cancelled. Note that this process simply reversed the first conditions noted above.

This process resulted in a list in which all the emails between DeMocker and Kennedy, on or between the specified dates, were checked. Those selected emails were exported from EnCase as Outlook message files (.msg or MSG).

The exported MSG files were then imported into Outlook 2003. Outlook stores emails, contacts, appointments and other items in a data file called a personal storage file (.pst or PST). A PST file was created to contain the above-selected emails, and given the name "Item 411 SD-CK Email Jan07-Jul08.pst". The PST file format was chosen so that the requested email files can be efficiently provided to, and analyzed by, other investigators involved in the case.

The above described process was repeated for each of the remaining requested examinations, modified for the respective dates, persons and Evidence Item. The PST file produced for each is noted below.

B) Email between DeMocker & Kennedy, 1/01/2007 – 7/03/2008, from Item 513
PST file name: Item 513 SD-CK Email Jan07-Jul08.pst.

C) Email between DeMocker & O'Non, 1/01/2007 – 10/23/2008, from Item 411
PST file name: Item 411 SD-Onon Email Jan07-Oct08.pst;

D) Email between DeMocker & O'Non, 1/01/2007 – 10/23/2008, from Item 301
PST file name: Item 301 SD-Onon Email Jan07-Oct08.pst;

The Outlook PST data files were then copied to CD discs. The Item 301 PST SD-Onon Email PST file was copied to its own CD disc; the Item 411 SD-Onon Email PST file was copied to its own CD disc; and the two PST files containing emails between DeMocker and Kennedy (SD-CK) were placed on a third CD disc. The discs were provided to Det. McDormett for further analysis.

Detective Steve Page, #5430
Yavapai County Sheriff's Office
Criminal Investigations Bureau

Peer Review:

The above listed report was peer reviewed for technical accuracy and content. The results listed in this report were reviewed with Detective Page to verify the statements made in this report accurately portray the forensic findings found using EnCase.

Detective P A. Lindvay, #5497

Yavapai County Sheriff's Office
Criminal Investigations Bureau
Computer Forensics Unit

Extracted Data Documentation

6249

AGENCY: Yavapai County Sheriff's Office
AGENCY DR#: 08-029129
CFU #: P0261
DPS Evidence DR#: 2008-723747
INVESTIGATOR: DETECTIVE JOHN MCDORMETT #5472
EXAMINER: DETECTIVE STEVE PAGE #5430
REPORT DATE: MARCH 31, 2010

Report Notes:

Digital media, consisting of CD(s) or DVD(s), accompany this report, and are an integral part of this report. A copy of this report is located on the digital media, and the digital report may contain hyperlinks to the supporting documentation. Any printed version of this report is incomplete by itself.

Requested Examination:

On or about 3/16/10 Sergeant Luis Huante and Detective Page discussed the various email reports and extracted email data developed in this case for analysis. As various previous requests, and the data extracted, were not fully inclusive of all the email from the evidence, Sergeant Huante requested that Detective Page extract all the identified email data from the below listed items, and to provide the extracted data to him for further analysis.

Evidence Items:

Item #		Description	Model No.
	Serial No.		
301	Dell Optiplex 745 computer, containing: One (1) Seagate Barracuda 160 GB SATA HDD	DCCY ST3160812AS	7P23SD1 5LSH1KS3
411	IBM ThinkPad Laptop, containing: One (1) Fujitsu 60.0GB SATA HDD	2623-D9U MHV2060BH	L3-A9400 NW06T6425FN9
512	256MB USB Flash Drive		
550-A	Lexar 256MB USB Flash Drive labeled "Photo"		
550-B	Lexar 256MB USB Flash Drive		
3108	Apple iPod 4GB, Silver	A1199	YM6347VFV8T
3110-R	CD, Labeled: "Backup Outlook.pst files"		

3110-T CD, Labeled: "Pre-XP File backups | [not lockable]"

Procedure:

The EnCase image files from the above listed Items were examined with versions of Guidance Software's EnCase 6 software and other applications used for viewing and managing computer files.

Computer Evidence:

The results of a search for email records previously run in EnCase were used in this examination for Items 301, 411 and 513. That search was documented in the 012910 Computer Evidence Forensic Report (Procedure section, under "General Email Searches", 4th paragraph). = 6171 1/29/2010

Item 301:

The root directory of the volume labeled "E:\" (Drive E as reported through EnCase) contained a folder named Documents and Settings, which contained a user folder named "se04788". An Outlook Offline Store file (.ost or OST) was located in "E:\Documents and Settings\se04788 \Local Settings\Application Data\Microsoft\Outlook. The Outlook OST file was examined with EnCase. It did not appear to contain any email data and was no further examination was conducted on the data.

The root directory of volume E contained a folder named "Users", which contained a single sub-folder named "se04788". The folder named "se04788" contained the user files for Steven DeMocker on Item 301. Within that folder, an Outlook PST file, named "archive Brooke.pst" was found. The PST file was exported for further analysis by other investigators.

Item 411:

The EnCase email search process identified Outlook Express email files. The email files were exported from EnCase as Outlook MSG files (.msg). The MSG files were then brought into Outlook 2003 and saved to an Outlook email container file (PST). The Outlook PST file was named "Item 411 Outlook Express Emails.pst". Outlook noted an error when importing five of the MSG files. The files could be opened individually outside of Outlook, and were therefore exported individually.

The EnCase email search process also identified four Outlook PST files on Item 411. The PST files were named "outlook.pst", "archive.pst", "backup.pst", and "backup.csv." The outlook.pst, archive.pst and backup.csv files were located in the directory "C:\Documents and Settings\Steven DeMocker\Local Settings\Application Data\Microsoft\Outlook\". This is the normal directory in which Outlook PST files are stored. The file named "backup.pst" was located in the directory "C:\Documents and Settings\Steven DeMocker\My Documents\My Pictures\Iraq\". This is not a normal directory in which Outlook PST files are stored. The .csv extension is not an Outlook PST file extension, however, the EnCase signature analysis process identified the file as an Outlook PST file. Signature analysis compares a file's hexadecimal header (first few bytes of a file) to a known hexadecimal header associated with a file extension (i.e. .pst). The name of the exported file "backup.csv" was changed to "backup.csv.pst." Re-naming the file allowed Outlook to recognize and open the file for further analysis. These four PST files were exported from EnCase.

The five Outlook PST files and five MSG files noted above were then copied to a CD disc for further analysis by other investigators.

Flash Memory Devices:

Item 512:

Item 512 was examined and a file named _ACKUP.PST was found in the root folder (i.e. "C:\") of the item. The file was exported from EnCase, and then brought into Outlook 2003. Outlook reported the file as not being a personal folders file (PST file). The exported file was then processed using Microsoft's Inbox Repair Tool (SCANPST.exe). The Inbox Repair Tool purpose and use is documented in the Microsoft Knowledge Base Article 287497. The Article notes that the Inbox Repair Tool can be used to recover folders and items from a corrupted Personal Folders (.pst) or offline folder (.ost) file.

The Inbox Repair Tool saved the original file as "_ACKUP.bak", and created a new PST file containing any recovered data, named "_ACKUP.PST". The program also created a log file of its processes. The new PST file was renamed "Item 512_ACKUP.PST" to uniquely identify it. The new PST file was then brought into Outlook 2003 and determined to contain contact (address book) data. The new PST file was copied to a CD for further analysis by other investigators; the original file (now "_ACKUP.bak") and the log file were also copied to the CD.

Item 550-A:

The EnCase email search process was run against Item 550-A to search for email data. The EnCase search identified Outlook Express email files. The email files were exported from EnCase as Outlook MSG files (.msg). The MSG files were then brought into Outlook 2003 and saved to an Outlook email container file (PST). The Outlook PST file was named "Item 550-A Email.pst". Outlook noted an error when importing three of the MSG files. The files could be opened individually outside of Outlook. The three MSG files were copied individually to the same export folder as the PST file. The Outlook PST and three MSG files were then copied to a CD disc for further analysis by other investigators.

Item 550-B:

The EnCase email search process was run against Item 550-B to search for email data. The item contained Outlook Express email files. The email files were exported from EnCase as Outlook MSG files (.msg). The MSG files were then brought into Outlook 2003 and saved to an Outlook email container file (PST). The Outlook PST file was named "Item 550-B Email.pst". Outlook noted an error when importing 29 of the MSG files. Twenty of the files could be opened individually outside of Outlook and were copied to the same export folder as the PST file. Nine of the files could not be opened, and were not copied out. The Outlook PST and 20 MSG files were then copied to a CD disc for further analysis by other investigators.

iPod Devices:

Item 3108 Notes:

The Outlook PST data carved from Unallocated Clusters on Item 3108 was brought into Outlook 2003. Outlook reported that errors were detected in the file. The file was then processed with the Inbox Repair Tool, which reported that the file could not be recognized. No furthe examination was conducted on the data.

Compact Discs:

Item 3110-R:

EnCase identified five Outlook PST files on the CD in a track labeled "(1) Backup-pst" as documented in the 012910 CD Forensic Report, to YCSO Evidence as Item 6175. All five files were named 'backup.pst'. The PST files were exported from EnCase. Each exported file was given a unique name for identification. The unique name included the Item name and the Physical Sector where the beginning of the file was located. The file 'backup.pst' located beginning at sector 557, for example, was exported with the new filename "Item 3110-R-C557-backup.pst". The five files were exported as:

Item 3110-R-C557-backup.pst
Item 3110-R-C2612-backup.pst
Item 3110-R-C4667-backup.pst
Item 3110-R-C4699-backup.pst
Item 3110-R-C4731-backup.pst

Once exported, each file was brought into Outlook 2003 to determine its contents. For the file "Item 3110-R-C557-backup.pst", Outlook reported that it detected errors in the file. For the remaining files, Outlook reported that each file was not a personal folders file. Each of the five files was processed using Microsoft's Inbox Repair Tool, as described for Item 512 above. The new PST files were each brought into Outlook and reviewed. The files "Item 3110-R-C557-backup.pst", "Item 3110-R-C4667-backup.pst" and "Item 3110-R-C4731-backup.pst" did not appear to contain any Outlook data. The files "Item 3110-R-C2612-backup.pst" and "Item 3110-R-C4699-backup.pst" contained Outlook-related data. The new PST files, now named "Item 3110-R-C2612-backup.pst" and "Item 3110-R-C4699-backup.pst", their original files (now with a ".bak" extension), and their associated log files were copied to a CD disc for further analysis by other investigators. The files that did not appear to contain any data were not copied.

Item 3110-T:

The Item contained one PST file named "backup.pst", located in the root directory. The file's size was approximately 2.7MB. The file was exported from EnCase, with the unique filename of "Item 3110-T backup.pst". The file was then brought into Outlook, which reported that it detected errors in the file. The file was processed with the Inbox Repair Tool as described previously. The new PST file was then brought into Outlook and reviewed. The new PST file did not appear to contain any Outlook data.

Steve Page #5430

Detective Steve Page, #5430
Yavapai County Sheriff's Office
Criminal Investigations Bureau

Peer Review:

The above listed report was peer reviewed for technical accuracy and content. The results listed in this report were reviewed with Detective Page to verify the statements made in this report accurately portray the forensic findings found using EnCase.

Paul Lindvay #5497

Detective P. A. Lindvay, #5497
AZ Department Of Public Safety
Computer Forensic Unit

Yavapai County Sheriff's Office
Criminal Investigations Bureau
Computer Forensics Unit

Extracted Data Documentation

6250

AGENCY: Yavapai County Sheriff's Office
AGENCY DR#: 08-029129
CFU #: P0261
DPS Evidence DR#: 2008-723747
INVESTIGATOR: DETECTIVE JOHN MCDORMETT #5472
EXAMINER: DETECTIVE STEVE PAGE #5430
REPORT DATE: MARCH 31, 2010

Report Notes:

Digital media, consisting of CD(s) or DVD(s), accompany this report, and are an integral part of this report. A copy of this report is located on the digital media, and the digital report may contain hyperlinks to the supporting documentation. Any printed version of this report is incomplete by itself.

Requested Examination:

On or about 3/16/10 Sergeant Luis Huante and Detective Page discussed the various email reports and extracted email data developed in this case for analysis. As various previous requests, and the data extracted, were not fully inclusive of all the email from the evidence, Sergeant Huante requested that Detective Page extract all the identified email data from the below listed items, and to provide the extracted data to him for further analysis.

Evidence Items:

Item #	Serial No.	Description	Model No.
301	Dell Optiplex 745 computer, containing: One (1) Seagate Barracuda 160 GB SATA HDD	DCCY ST3160812AS	7P23SD1 5LSH1KS3
411	IBM ThinkPad Laptop, containing: One (1) Fujitsu 60.0GB SATA HDD	2623-D9U MHV2060BH	L3-A9400 NW06T6425FN9
512	256MB USB Flash Drive		
550-A	Lexar 256MB USB Flash Drive labeled "Photo"		
550-B	Lexar 256MB USB Flash Drive		
3108	Apple iPod 4GB, Silver	A1199	YM6347VFV8T
3110-R	CD, Labeled: "Backup Outlook.pst files"		

3110-T CD, Labeled: "Pre-XP File backups | [not lockable]"

Procedure:

The EnCase image files from the above listed Items were examined with versions of Guidance Software's EnCase 6 software and other applications used for viewing and managing computer files.

Computer Evidence:

The results of a search for email records previously run in EnCase were used in this examination for Items 301, 411 and 513. That search was documented in the 012910 Computer Evidence Forensic Report (Procedure section, under "General Email Searches", 4th paragraph).

Item 301:

The root directory of the volume labeled "E:\" (Drive E as reported through EnCase) contained a folder named Documents and Settings, which contained a user folder named "se04788". An Outlook Offline Store file (.ost or OST) was located in "E:\Documents and Settings\se04788 \Local Settings\Application Data\Microsoft\Outlook. The Outlook OST file was examined with EnCase. It did not appear to contain any email data and was no further examination was conducted on the data.

The root directory of volume E contained a folder named "Users", which contained a single sub-folder named "se04788". The folder named "se04788" contained the user files for Steven DeMocker on Item 301. Within that folder, an Outlook PST file, named "archive Brooke.pst" was found. The PST file was exported for further analysis by other investigators.

Item 411:

The EnCase email search process identified Outlook Express email files. The email files were exported from EnCase as Outlook MSG files (.msg). The MSG files were then brought into Outlook 2003 and saved to an Outlook email container file (PST). The Outlook PST file was named "Item 411 Outlook Express Emails.pst". Outlook noted an error when importing five of the MSG files. The files could be opened individually outside of Outlook, and were therefore exported individually.

The EnCase email search process also identified four Outlook PST files on Item 411. The PST files were named "outlook.pst", "archive.pst", "backup.pst", and "backup.csv." The outlook.pst, archive.pst and backup.csv files were located in the directory "C:\Documents and Settings\Steven DeMocker\Local Settings\Application Data\Microsoft\Outlook\". This is the normal directory in which Outlook PST files are stored. The file named "backup.pst" was located in the directory "C:\Documents and Settings\Steven DeMocker\My Documents\My Pictures\Iraq\". This is not a normal directory in which Outlook PST files are stored. The .csv extension is not an Outlook PST file extension, however, the EnCase signature analysis process identified the file as an Outlook PST file. Signature analysis compares a file's hexadecimal header (first few bytes of a file) to a known hexadecimal header associated with a file extension (i.e. .pst). The name of the exported file "backup.csv" was changed to "backup.csv.pst." Re-naming the file allowed Outlook to recognize and open the file for further analysis. These four PST files were exported from EnCase.

The five Outlook PST files and five MSG files noted above were then copied to a CD disc for further analysis by other investigators.

Flash Memory Devices:

Item 512:

Item 512 was examined and a file named _ACKUP.PST was found in the root folder (i.e. "C:\") of the item. The file was exported from EnCase, and then brought into Outlook 2003. Outlook reported the file as not being a personal folders file (PST file). The exported file was then processed using Microsoft's Inbox Repair Tool (SCANPST.exe). The Inbox Repair Tool purpose and use is documented in the Microsoft Knowledge Base Article 287497. The Article notes that the Inbox Repair Tool can be used to recover folders and items from a corrupted Personal Folders (.pst) or offline folder (.ost) file.

The Inbox Repair Tool saved the original file as "_ACKUP.bak", and created a new PST file containing any recovered data, named "_ACKUP.PST". The program also created a log file of its processes. The new PST file was renamed "Item 512_ACKUP.PST" to uniquely identify it. The new PST file was then brought into Outlook 2003 and determined to contain contact (address book) data. The new PST file was copied to a CD for further analysis by other investigators; the original file (now "_ACKUP.bak") and the log file were also copied to the CD.

Item 550-A:

The EnCase email search process was run against Item 550-A to search for email data. The EnCase search identified Outlook Express email files. The email files were exported from EnCase as Outlook MSG files (.msg). The MSG files were then brought into Outlook 2003 and saved to an Outlook email container file (PST). The Outlook PST file was named "Item 550-A Email.pst". Outlook noted an error when importing three of the MSG files. The files could be opened individually outside of Outlook. The three MSG files were copied individually to the same export folder as the PST file. The Outlook PST and three MSG files were then copied to a CD disc for further analysis by other investigators.

Item 550-B:

The EnCase email search process was run against Item 550-B to search for email data. The item contained Outlook Express email files. The email files were exported from EnCase as Outlook MSG files (.msg). The MSG files were then brought into Outlook 2003 and saved to an Outlook email container file (PST). The Outlook PST file was named "Item 550-B Email.pst". Outlook noted an error when importing 29 of the MSG files. Twenty of the files could be opened individually outside of Outlook and were copied to the same export folder as the PST file. Nine of the files could not be opened, and were not copied out. The Outlook PST and 20 MSG files were then copied to a CD disc for further analysis by other investigators.

iPod Devices:

Item 3108 Notes:

The Outlook PST data carved from Unallocated Clusters on Item 3108 was brought into Outlook 2003. Outlook reported that errors were detected in the file. The file was then processed with the Inbox Repair Tool, which reported that the file could not be recognized. No further examination was conducted on the data.

Compact Discs:

Item 3110-R:

EnCase identified five Outlook PST files on the CD in a track labeled "(1) Backup-pst" as documented in the 012910 CD Forensic Report, to YCSO Evidence as Item 6175. All five files were named 'backup.pst'. The PST files were exported from EnCase. Each exported file was given a unique name for identification. The unique name included the Item name and the Physical Sector where the beginning of the file was located. The file 'backup.pst' located beginning at sector 557, for example, was exported with the new filename "Item 3110-R-C557-backup.pst". The five files were exported as:

Item 3110-R-C557-backup.pst
Item 3110-R-C2612-backup.pst
Item 3110-R-C4667-backup.pst
Item 3110-R-C4699-backup.pst
Item 3110-R-C4731-backup.pst

Once exported, each file was brought into Outlook 2003 to determine its contents. For the file "Item 3110-R-C557-backup.pst", Outlook reported that it detected errors in the file. For the remaining files, Outlook reported that each file was not a personal folders file. Each of the five files was processed using Microsoft's Inbox Repair Tool, as described for Item 512 above. The new PST files were each brought into Outlook and reviewed. The files "Item 3110-R-C557-backup.pst", "Item 3110-R-C4667-backup.pst" and "Item 3110-R-C4731-backup.pst" did not appear to contain any Outlook data. The files "Item 3110-R-C2612-backup.pst" and "Item 3110-R-C4699-backup.pst" contained Outlook-related data. The new PST files, now named "Item 3110-R-C2612-backup.pst" and "Item 3110-R-C4699-backup.pst", their original files (now with a ".bak" extension), and their associated log files were copied to a CD disc for further analysis by other investigators. The files that did not appear to contain any data were not copied.

Item 3110-T:

The Item contained one PST file named "backup.pst", located in the root directory. The file's size was approximately 2.7MB. The file was exported from EnCase, with the unique filename of "Item 3110-T backup.pst". The file was then brought into Outlook, which reported that it detected errors in the file. The file was processed with the Inbox Repair Tool as described previously. The new PST file was then brought into Outlook and reviewed. The new PST file did not appear to contain any Outlook data.

Steve Page #5430

Detective Steve Page, #5430
Yavapai County Sheriff's Office
Criminal Investigations Bureau

Peer Review:

The above listed report was peer reviewed for technical accuracy and content. The results listed in this report were reviewed with Detective Page to verify the statements made in this report accurately portray the forensic findings found using EnCase.

Paul Lindvay #5497

Detective P. A. Lindvay, #5497
AZ Department Of Public Safety
Computer Forensic Unit

Procedure:

The EnCase image files from the above listed Items were examined with versions of Guidance Software's EnCase 6 software and other applications used for viewing and managing computer files.

Computer Evidence:

The results of a search for email records previously run in EnCase were used in this examination for Items 301, 411 and 513. That search was documented in the 012910 Computer Evidence Forensic Report (Procedure section, under "General Email Searches", 4th paragraph).

Item 301:

The root directory of the volume labeled "E:\" (Drive E as reported through EnCase) contained a folder named Documents and Settings, which contained a user folder named "se04788". An Outlook Offline Store file (.ost or OST) was located in "E:\Documents and Settings\se04788\Local Settings\Application Data\Microsoft\Outlook. The Outlook OST file was examined with EnCase. It did not appear to contain any email data and was no further examination was conducted on the data.

The root directory of volume E contained a folder named "Users", which contained a single sub-folder named "se04788". The folder named "se04788" contained the user files for Steven DeMocker on Item 301. Within that folder, an Outlook PST file, named "archive Brooke.pst" was found. The PST file was exported for further analysis by other investigators.

Item 411:

The EnCase email search process identified Outlook Express email files. The email files were exported from EnCase as Outlook MSG files (.msg). The MSG files were then brought into Outlook 2003 and saved to an Outlook email container file (PST). The Outlook PST file was named "Item 411 Outlook Express Emails.pst". Outlook noted an error when importing five of the MSG files. The files could be opened individually outside of Outlook, and were therefore exported individually.

The EnCase email search process also identified four Outlook PST files on Item 411. The PST files were named "outlook.pst", "archive.pst", "backup.pst", and "backup.csv." The outlook.pst, archive.pst and backup.csv files were located in the directory "C:\Documents and Settings\Steven DeMocker\Local Settings\Application Data\Microsoft\Outlook\". This is the normal directory in which Outlook PST files are stored. The file named "backup.pst" was located in the directory "C:\Documents and Settings\Steven DeMocker\My Documents\My Pictures\Iraq\". This is not a normal directory in which Outlook PST files are stored. The .csv extension is not an Outlook PST file extension, however, the EnCase signature analysis process identified the file as an Outlook PST file. Signature analysis compares a file's hexadecimal header (first few bytes of a file) to a known hexadecimal header associated with a file extension (i.e. .pst). The name of the exported file "backup.csv" was changed to "backup.csv.pst." Re-naming the file allowed Outlook to recognize and open the file for further analysis. These four PST files were exported from EnCase.

The five Outlook PST files and five MSG files noted above were then copied to a CD disc for further analysis by other investigators.

Flash Memory Devices:

Item 512:

Item 512 was examined and a file named _ACKUP.PST was found in the root folder (i.e. "C:\") of the item. The file was exported from EnCase, and then brought into Outlook 2003. Outlook reported the file as not being a personal folders file (PST file). The exported file was then processed using Microsoft's Inbox Repair Tool (SCANPST.exe). The Inbox Repair Tool purpose and use is documented in the Microsoft Knowledge Base Article 287497. The Article notes that the Inbox Repair Tool can be used to recover folders and items from a corrupted Personal Folders (.pst) or offline folder (.ost) file.

The Inbox Repair Tool saved the original file as "_ACKUP.bak", and created a new PST file containing any recovered data, named "_ACKUP.PST". The program also created a log file of its processes. The new PST file was renamed "Item 512_ACKUP.PST" to uniquely identify it. The new PST file was then brought into Outlook 2003 and determined to contain contact (address book) data. The new PST file was copied to a CD for further analysis by other investigators; the original file (now "_ACKUP.bak") and the log file were also copied to the CD.

Item 550-A:

The EnCase email search process was run against Item 550-A to search for email data. The EnCase search identified Outlook Express email files. The email files were exported from EnCase as Outlook MSG files (.msg). The MSG files were then brought into Outlook 2003 and saved to an Outlook email container file (PST). The Outlook PST file was named "Item 550-A Email.pst". Outlook noted an error when importing three of the MSG files. The files could be opened individually outside of Outlook. The three MSG files were copied individually to the same export folder as the PST file. The Outlook PST and three MSG files were then copied to a CD disc for further analysis by other investigators.

Item 550-B:

The EnCase email search process was run against Item 550-B to search for email data. The item contained Outlook Express email files. The email files were exported from EnCase as Outlook MSG files (.msg). The MSG files were then brought into Outlook 2003 and saved to an Outlook email container file (PST). The Outlook PST file was named "Item 550-B Email.pst". Outlook noted an error when importing 29 of the MSG files. Twenty of the files could be opened individually outside of Outlook and were copied to the same export folder as the PST file. Nine of the files could not be opened, and were not copied out. The Outlook PST and 20 MSG files were then copied to a CD disc for further analysis by other investigators.

iPod Devices:

Item 3108 Notes:

The Outlook PST data carved from Unallocated Clusters on Item 3108 was brought into Outlook 2003. Outlook reported that errors were detected in the file. The file was then processed with the Inbox Repair Tool, which reported that the file could not be recognized. No further examination was conducted on the data.

Compact Discs:

Item 3110-R:

EnCase identified five Outlook PST files on the CD in a track labeled "(1) Backup-pst" as documented in the 012910 CD Forensic Report, to YCSO Evidence as Item 6175. All five files were named 'backup.pst'. The PST files were exported from EnCase. Each exported file was given a unique name for identification. The unique name included the Item name and the Physical Sector where the beginning of the file was located. The file 'backup.pst' located beginning at sector 557, for example, was exported with the new filename "Item 3110-R-C557-backup.pst". The five files were exported as:

Item 3110-R-C557-backup.pst
Item 3110-R-C2612-backup.pst
Item 3110-R-C4667-backup.pst
Item 3110-R-C4699-backup.pst
Item 3110-R-C4731-backup.pst

Once exported, each file was brought into Outlook 2003 to determine its contents. For the file "Item 3110-R-C557-backup.pst", Outlook reported that it detected errors in the file. For the remaining files, Outlook reported that each file was not a personal folders file. Each of the five files was processed using Microsoft's Inbox Repair Tool, as described for Item 512 above. The new PST files were each brought into Outlook and reviewed. The files "Item 3110-R-C557-backup.pst", "Item 3110-R-C4667-backup.pst" and "Item 3110-R-C4731-backup.pst" did not appear to contain any Outlook data. The files "Item 3110-R-C2612-backup.pst" and "Item 3110-R-C4699-backup.pst" contained Outlook-related data. The new PST files, now named "Item 3110-R-C2612-backup.pst" and "Item 3110-R-C4699-backup.pst", their original files (now with a ".bak" extension), and their associated log files were copied to a CD disc for further analysis by other investigators. The files that did not appear to contain any data were not copied.

Item 3110-T:

The Item contained one PST file named "backup.pst", located in the root directory. The file's size was approximately 2.7MB. The file was exported from EnCase, with the unique filename of "Item 3110-T backup.pst". The file was then brought into Outlook, which reported that it detected errors in the file. The file was processed with the Inbox Repair Tool as described previously. The new PST file was then brought into Outlook and reviewed. The new PST file did not appear to contain any Outlook data.

Steve Page #5430

Detective Steve Page, #5430
Yavapai County Sheriff's Office
Criminal Investigations Bureau

Peer Review:

The above listed report was peer reviewed for technical accuracy and content. The results listed in this report were reviewed with Detective Page to verify the statements made in this report accurately portray the forensic findings found using EnCase.

Paul Lindvay #5497

Detective P. A. Lindvay, #5497
AZ Department Of Public Safety
Computer Forensic Unit

Arizona Department of Public Safety
Computer Forensic Unit
Forensic Report

AGENCY: Yavapai County Sheriff's Office
AGENCY DR #: 09-003846
DPS EVIDENCE #: 2009-703853
CFU REQUEST #: P0364
INVESTIGATOR: Detective J. McDormett
EXAMINER: Sergeant R. Arthur #3439, Arizona Dept. of Public Safety

Requested Examination:

I was requested by Yavapai County Sheriff's Office (YCSO) to conduct an examination on Item 1 listed below for evidence related to the deaths of James Knapp and Carol Kennedy. The search warrant authorizing examination of the below listed item was provided with the request.

Evidence Item:

Item Number:	1
Item Description:	Dell Laptop Computer
Model Number:	C640
Serial Number:	CN04P2404815527T0403
HDD Description:	Hitachi Model #DK23DA-30F, 30.1GB IDE hard drive, Serial# LGVD12WN7X

Protocol:
Completed By: Sergeant R. Arthur #3439

The above listed item was delivered to the Arizona Regional Computer Forensics Lab by YCSO Sergeant L. Huarte on 1/30/09 at 1015 hours.

I conducted a physical inspection of Item 1 and documented its physical condition with photographs. During this examination, I checked the CD/DVD tray and found it to be empty. The BIOS time clock was checked for accuracy with the current date and time. The BIOS clock reported a date/time of 2/1/2009 / 11:52:39 on 2/1/2009 at 1149 hours.

I removed the hard drive from Item 1 and attached the hard drive to a government computer via a Digital Intelligence IDE writeblocking device. This was done to prevent any alterations to the source media during imaging. The item was successfully imaged using Guidance Software's EnCase software, version 6.12. The imaging process completed successfully with matching acquisition and verification MD5 hash values.

Arizona Department of Public Safety
Computer Forensic Unit
Forensic Report

Examination Findings:

ITEM 1

The operating system installed on Item 1 is Windows 2000 Service Pack 3, which was installed on 08/30/2002 at 1740 hours (local time). The operating system shows the Registered Organization as "Embry Riddle Aeronautical University" and the Registered Owner as "Development Laptop". The operating system's time zone is set as "US Mountain Standard Time" with daylight savings time turned off. The system contains four user accounts; "Administrator", "Guest", "Ferrell", and "KnappJ". The "Ferrell" and "Guest" accounts have never been logged into according to the computer registry files. The "Administrator" account has been logged into 23 times with the last login occurring on 09/25/2002 at 17:01:50 UTC. The "Administrator" account appears to require a password for login. The "knappj" account was logged into a total of 1766 times with the last login occurring on 01/04/2009 at 19:06:52 UTC. The "knappj" account appears to require a password for login. The previously mentioned information was obtained using AccessData's Registry Viewer version 1.5.4.44 on the Windows Registry files stored on Item 1.

The images in the allocated space of Item 1 were examined using EnCase's gallery view for images of interest. Six items of possible evidentiary interest were located and bookmarked. The bookmarked images can be viewed here.

The EnCase Case Processor File Finder script was run to locate Joint Photography Experts Group (JPG) images in the unallocated space of the item. EnCase recovered 990 JPG images from unallocated space of Item 1. The recovered images were reviewed and no items of evidentiary interest were located.

EnCase was utilized to locate and review document files such as; Microsoft Office documents, Adobe PDF documents, and text documents. Thirty-eight (38) files were bookmarked as possible items of evidence. These files can be reviewed in the EnCase Bookmark Report.

AccessData's Forensic Tool Kit (FTK) was utilized to located and review email from Item 1. Two hundred sixty-three (263) emails were bookmarked as possible emails of interest. These emails can be reviewed in the FTK Email of Interest Report.

A keyword search was conducted using EnCase for the following terms provided by Yavapai County Sheriff's Office investigators. Items of evidentiary value located were documented in the FTK Email of Interest Report or the EnCase Bookmark Report:

ckennedy@cableone.net – No items of evidentiary value were located.

carolkennedy66@gmail.com – No items of evidentiary value were located.

virginiacarolkennedy@gmail.com – No items of evidentiary value were located.

Arizona Department of Public Safety
Computer Forensic Unit
Forensic Report

sdem@cableone.net – There were a total of 6 search hits related to this search term, all of which were related to a series of 3 emails between Carol Kennedy and James Knapp on November 13, 2007 and November 15, 2007. The emails were titled; "can you be my objective ears coach?", "RE: can you be my objective ears coach?", and "FW can you be my objective ears coach?" Refer to Email of Interest report.

democker@cableone.net – There were a total of 6 search hits related to this search term, all of which were related to the same 3 emails between Carol Kennedy and James Knapp as documented in the previous paragraph.

steven.democker@gmail.com – No items of evidentiary value were located.

Democker – 3 items (documents) were bookmarked as possible items of evidentiary value in the EnCasc Bookmark Rcport.

Alex Knapp – 1 item (document) was bookmarked as a possible item of evidentiary value in the EnCase Bookmark Report.

Jay Knapp – 1 item (document) was bookmarked as a possible item of evidentiary value in the EnCase Bookmark Report.

Ann Saxerud – 8 items (emails/documents) were bookmarked as possible items of evidentiary value in the EnCase Bookmark Report and the FTK Email of Interest Report.

Steve Democker – No items of evidentiary value were located.

Benzodiazepines – 1 item (document) was bookmarked as a possible item of evidentiary value in the EnCase Bookmark Report.

Nordiazepam – No items of evidentiary value were located.

Chlordiazepoxide – No items of evidentiary value were located.

Tramadol – No items of evidentiary value were located.

Nortramadol – No items of evidentiary value were located.

Norsertraline – No items of evidentiary value were located.

Promethazine – No items of evidentiary value were located.

Zolpidem – No items of evidentiary value were located.

Oxycotin – No items of evidentiary value were located.

Oxycodone – No items of evidentiary value were located.